

### Listing of Claims:

1. (Currently Amended) A cryptographic method of anonymously signing a message by a member of a group comprising [[n]] a plurality of members each equipped with calculation means (25) and associated storage means (24), ~~which method is characterized in that it comprises the following initial steps at the time of constituting the group, the method initially comprising:~~

~~[[ -]]~~ a first step of calculating, ~~in which~~ at first calculation means of a trusted authority, ~~calculate~~ a pair of asymmetric keys (30, 31) common to the members of the group and comprising a common public key (30) and a common private key; (31) ~~(operation-1)~~[[,]]

~~[[ -]]~~ a second step of calculating, ~~at in which~~ the first calculation means of the trusted authority, ~~calculate~~ a group public key (32) associated with the members of the group; ~~(operation-2)~~[[,]]

~~[[ -]]~~ a third step of ~~in which, for each member~~[[,]] calculating, during an interaction between the calculation means of the trusted authority and the calculation means of the member, a group private key (33) ~~is calculated (operation-3) and stored (operation-4) for each member of the group and storing the private key~~ in the storage means (24) of the each member, each group private key (33) being associated with the group public key (32) and being different for each member of the group;[[,]]

~~[[ -]]~~ a fourth step of determining, ~~in which~~ at the first calculation means of the trusted authority, ~~determine~~ as many symmetrical secret keys (34) as there are members of the group; ~~(operation-5)~~[[,]] and

~~[[ -]]~~ a fifth step of encrypting, ~~at in which~~ the first calculation means of the trusted authority, (20) ~~encrypt~~ the common private key (31) using each of the

symmetrical secret keys (34<sub>i</sub>) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members; ~~(operation-6)~~[[,]]

~~and in that it comprises the following steps on each revocation within of a member from the group, the method further comprising:~~

[[~~-~~]] a sixth step of modifying, ~~in which~~ at the first calculation means of the trusted authority, ~~(20)~~ modify the pair of ~~common~~ asymmetric keys common to the group (31) to ~~determine~~ create [[a]] an up-to-date common public key (30) and [[a]] an up-to-date common private key; ~~(31) that are up-to-date (operation 8)~~[[,]]

[[~~-~~]] a seventh step of encrypting, ~~in which~~ at the first calculation means of the trusted authority, ~~(20)~~ encrypt the up-to-date common private key (31) using each of the symmetrical secret keys (34<sub>i</sub>) to obtain as many encrypted forms of the up-to-date common private key (31) as there are non-revoked members; and (operation-9)[[,]]

~~and in that the method comprises the following steps on the~~ when a non-revoked group member anonymously signing (operation-10) signs a message having to be sent to an addressee, the method further comprising:

[[~~-~~]] an eighth step of updating ~~in which~~ the common private key (31) stored ~~by~~ in the storage means (24) of the signing member is updated ~~(operation 11)~~ only if one ~~of the~~ encrypted values value of the up-to-date common private key (31) may be decrypted using the symmetrical secret key (34<sub>i</sub>) stored in the ~~member's storage means~~ of the signing member; ~~(24)~~[[,]]

[[~~-~~]] a ninth step of calculating, ~~at the~~ ~~in which the member's calculation means~~ of the signing member, ~~(25)~~ calculate ~~(operation-12)~~ an anonymous

signature of the message using its the group private key for the signing member;  
(33<sub>+</sub>)[[.]] and

[[ - ]] a tenth step of calculating, at in which the member's the calculation  
means of the signing member, (24) calculate (operation 13) an additional  
signature of the a combination comprising the message and the anonymous  
signature using the member's up-to-date common private key (31) of the signing  
member.

2. (Currently Amended) [[A]] The cryptographic anonymous signature method according  
to claim 1, wherein the group is constituted at a date t1 and the method further comprising the  
following operations comprises:

[[ - ]] during the first step associating, at the first calculation means, associate  
the common private key (31) with an update updated date equal to t1; (operation  
14)[[.]] and

[[ - ]] during the third step storing, at the storage means (24) of each member,  
store the update the updated date of the common private key; (operation 15)[[.]]

wherein the following operation is executed at the time of each revocation  
within the group at a date t2:

[[ - ]] during the sixth step modifying, at the first calculation means of the  
trusted authority, (20) modify the update the updated date to determine an update  
updated date equal to the date t2; and (operation 16)[[. and]]

wherein the following operation is executed on each anonymous signing by  
the member of the group of [[a]] the message having to be sent to [[an]] the  
addressee:

[[ -]] during the eighth step, the common private key stored in the ~~member's~~ storage means of the signing member (24) is updated (~~operation 11~~) only if the ~~update~~ updated date ( $D_i$ ) in the ~~member's~~ storage means of the signing member (24) is also different from the ~~update~~ updated date ( $D$ ) of the up-to-date common private key (31) updated by the first calculation means of the trusted authority.

3. (Currently Amended) [[A]] The cryptographic anonymous signature method according to claim 1, further comprising: ~~the following operations~~[[ :]]

[[ -]] during the third step calculating, at the first calculation means, ~~calculate~~ for each member of the group an identifier ( $35_i$ ) of the member for each member of the group (~~operation 3~~) and storing the identifier ( $35_i$ ) of the each member of the group is stored in the ~~member's~~ storage means of each member; and (24) (~~operation 4~~)[[ , and]]

calculating, ~~the following operation on each revocation within the group~~[[ : -]] at the first calculation means of the trusted authority (20) ~~calculate~~ an identifier ( $35_i$ ) for each new member of the group on each revocation within the group.

4. (Currently Amended) [[A]] The cryptographic method according to claim 3, ~~of anonymously signing a message, wherein the steps further comprise~~ further comprising:

[[ -]] during the third step storing, at storage means ( $36$ ) connected to the first calculation means of the trusted authority, ( $20$ ) ~~store~~ the symmetrical secret key ( $34_i$ ) of each member, the group public key ( $32$ ), the public key ( $30$ ) common to the members of the group, each of the encrypted forms of the common private key ( $31$ ), and each of the identifiers ( $35_i$ ), each encrypted form of the common

private key (31) being associated with one of the identifiers; and (35);[[,]]

~~and further comprising the following operation~~ for each modification of the composition of the group that corresponds to a revocation of one of the members of the group, the method further comprising:

[[ - ]] removing the secret key (34;) of that member from the storage means (36) connected to the first calculation means of the trusted authority; and (20)[[,]]

~~and further comprising the following operations~~ to update the common private key (31) stored in the ~~member's~~ storage means (24) of the member, the method further comprising:

[[ - ]] reading, at the ~~member's~~ calculation means of the member, (25) ~~read~~ ~~the different~~ the encrypted form (31) of the common private key stored in the storage means (36) connected to the first calculation means of the trusted authority (20) and associated with the identifier (35;) of the member;[[,]] and

[[ - ]] decrypting, at the ~~member's~~ calculation means of the member, (25) ~~decrypt the different~~ the encrypted form of the common private key (31) previously read using the secret key (34;) stored in the ~~member's~~ storage means of the member. (24)[[,]]

5. (Currently Amended) [[A]] The cryptographic method according to claim 1 of ~~anonymously signing a message,~~ wherein the ~~initial steps~~ further ~~comprise~~ further comprising:

[[ - ]] during the third step storing, at storage means (36) connected to the first calculation means of the trusted authority, (20) ~~store~~ the secret key of each member, the pair of asymmetric keys (30, 31) common to the members of the group, and the group public key; and (32)[[,]]

~~and further comprising the following operation~~ on each modification of the composition of the group that corresponds to a revocation within the group:

[[~~-~~]] eliminating the secret key of the a revoked member ~~is eliminated~~ from the storage means (36) connected to the first calculation means of the trusted authority; and (20)[[,]]

~~and further comprising the following operations~~ to update the common private key (31) ~~in a member's~~ in the storage means of the member, the method further comprising: (24)[[:]]

[[~~-~~]] reading, at the ~~member's~~ calculation means (25) of the member read the ~~different~~ encrypted forms of the common private key (31) in the storage means (36) connected to the first calculation means of the trusted authority; (20)[[,]] and

[[~~-~~]] using, at the ~~member's~~ calculation means of the member, use the secret key (34<sub>+</sub>) in the ~~member's~~ storage means (24) of the member to decrypt the ~~different~~ encrypted forms of the common private key (31).

6. - 9 (Canceled)

10. (Currently Amended) A cryptographic system for anonymously signing a digital message, ~~by implementing a method according to claim 1, characterized in that it comprises at least the system comprising:~~

[[~~-~~]] first calculation means (20) for calculating (~~operations 1, 2~~) at least one of said a pair of asymmetric keys (30, 31) common to the members of the a group of a plural members and said a group public key (32) associated with the

group, for calculating ~~(operation-3)~~ said group private key ~~(33<sub>i</sub>)~~ for each member during interaction with ~~the member's~~ a calculation means (25) of the each member, each said group private key ~~(33<sub>i</sub>)~~ for each member being associated with said group public key (32) and being different for each member of the group, for creating ~~determining (operation-5)~~ as many ~~of said~~ symmetrical secret keys (34<sub>i</sub>) as there are members of the group, and encrypting ~~(operation-6)~~ said a common private key (31) of said asymmetrical keys common to said members of the group using each of said symmetrical secret keys (34<sub>i</sub>) to obtain as many encrypted forms of said common private key (31) as there are non-revoked members; and

a smart card associated with each member as many smart cards (21<sub>i</sub>) as there are members in the group, wherein each smart card comprises comprising:

means (24) for storing said common private key (31) ~~common to the members of the group~~, said group private key ~~(33<sub>i</sub>)~~ of the each member, and said symmetrical secret key (34<sub>i</sub>) assigned to the each member;[[,]]

means (25) for updating said common private key (31) stored in the ~~member's~~ storage means of the each member (34) to update ~~(operation-11)~~ said common private key (31) only if one ~~of the~~ encrypted values value of said common private key (31) calculated by said first calculation means (20) ~~of the apparatus~~ may be decrypted using said symmetrical secret key (34<sub>i</sub>) in said ~~member's~~ storage means of the each member; and (24), and

calculation means (25) for calculating ~~(operation-12)~~ an anonymous signature for a message using its said group private key ~~(33<sub>i</sub>)~~ of the each member and for calculating ~~(operation-13)~~ an additional signature for the a combination

comprising the message and the anonymous signature using ~~the member's~~ said common private key (31).

11. (Currently Amended) ~~[[An]] A computer-readable medium encoded with a computer program executed by a computer which causes article of manufacture for use in a computer system, having a computer usable medium, to perform a cryptographic method of anonymously~~ anonymous signing of a message by a member of a group comprising a plurality of ~~[[n]]~~ members each equipped with calculation means (25) and associated storage means, (24), ~~wherein the computer usable medium includes a computer readable code means for causing the computer program comprising:~~

(i) program code for, at creation of the time of constituting the group:

calculating (~~operation 1~~), with a first calculation means of a trusted authority, a pair of asymmetric keys (30, 31) common to the members of the group and comprising a common public key (30) and a common private key (31),

calculating (~~operation 2~~), with the first calculation means of the trusted authority, a group public key (32) associated with the group of members;[[,]]

calculating (~~operation 3~~), ~~for each member~~, during an interaction between the calculation means of the trusted authority and ~~the~~ a calculation means of the member, a group private key (33<sub>i</sub>) for each member of the group[[,]] and storing (~~operation 4~~) said group private key (33<sub>i</sub>) in the a storage means (24) of the each member, each group private key (33<sub>i</sub>) being associated with the



group public key (32) and being different for each member of the group;<sub>i</sub>[[,]]

determining (~~operation-5~~), with the first calculation means, as many symmetrical secret keys (34;<sub>i</sub>) as there are members of the group;<sub>i</sub>[[,]] and

encrypting (~~operation-6~~), with the first calculation means (20), the common private key (31) using each of the symmetrical secret keys (34;<sub>i</sub>) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members;

(ii) program code for, on each member revocation within from the group:

modifying (~~operation-8~~), with the first calculation means (20), the pair of ~~common~~ asymmetric keys (31) common to the members of the group to ~~determine~~ create [[a]] an up-to-date common public key (30) and [[a]] an up-to-date common private key;<sub>i</sub> (31) ~~that are up-to-date~~[[,]]

encrypting (~~operation-9~~), with the first calculation means (20), the up-to-date common private key (31) of the pair of asymmetric keys common to the members of the group using each of the secret keys (34;<sub>i</sub>) to obtain as many encrypted forms of the up-to-date common private key (31) as there are non-revoked members; and

(iii) program code for, when a on-the group member anonymously signing

(~~operation-10~~) signs a message having to be sent to an addressee:

updating (~~operation-11~~) the common private key (31) stored by the storage means (24) of the signing member only if one of the encrypted values value of the up-to-date common private key (31) may be decrypted using the symmetrical secret key (34<sub>i</sub>) in the member's storage means of the signing member; (24)[[,]]

calculating (~~operation-12~~), with the member's calculation means of the signing member (25), an anonymous signature of the message using it's the group private key (33<sub>+</sub>), and

calculating (~~operation-13~~), with the member's calculation means of the signing member (24), an additional signature of the a combination comprising the message and the anonymous signature using the member's up-to-date common private key (31) of the signing member.